



INVESTOR IN PEOPLE

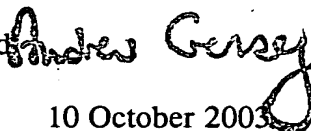
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

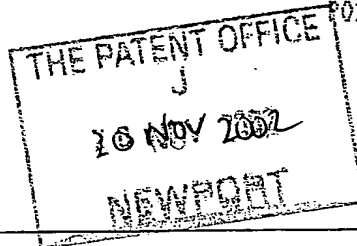
Signed 
Dated 10 October 2003

THIS PAGE BLANK (USPTO)

20NOV02 E764913-1 002759
01/7700 0.00-0227065.0

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)



The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference

C1504

2. Patent application number

(The Patent Office will fill in this part)

0227065.0

3. Full name, address and postcode of the or of each applicant (underline all surnames)

FUJITSU SERVICES LIMITED
26 Finsbury Square, London EC2A 1SL

Patents ADP number (if you know it)

If the applicant is a corporate body, give the country/state of its incorporation

ENGLAND

8347395002

4. Title of the invention

MULTIPLE NETWORK ACCESS

5. Name of your agent (if you have one)

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

D C Guyatt
Intellectual Property Department
Fujitsu Services Limited
Observatory House
Windsor Road
Slough SL1 2EY

8347395003

Patents ADP number (if you know it)

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country

Priority application number
(if you know it)

Date of filing
(day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description

Claim(s)

Abstract

Drawing(s)

§ 7
1
1
2 x 2

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (Patents Form 7/77)

Request for preliminary examination and search (Patents Form 9/77)

Request for substantive examination (Patents Form 10/77)

Any other documents (please specify)

—
—
1 + 2
1
—

11. I/We request the grant of a patent on the basis of this application.

Signature

D. C. Guyatt

Date

19/11/2002

12. Name and daytime telephone number of person to contact in the United Kingdom

D. C. Guyatt
01753 604388

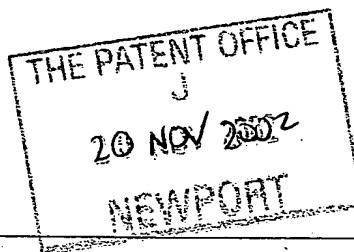
Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

**Statement of inventorship and of
right to grant of a patent**



The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference C1504

2. Patent application number
(if you know it)

0227065.0

3. Full name of the or of each applicant
FUJITSU SERVICES LIMITED

4. Title of the invention

MULTIPLE NETWORK ACCESS

5. State how the applicant(s) derived the right
from the inventor(s) to be granted a patent

BY REASON OF EMPLOYMENT

6. How many, if any, additional Patents Forms
7/77 are attached to this form?
(see note (c))

7. I/We believe that the person(s) named over the page (and on
any extra copies of this form) is/are the inventor(s) of the invention
which the above patent application relates to.

Signature

D.C. Guyatt

Date

19/11/2002

8. Name and daytime telephone number of
person to contact in the United Kingdom

D.C. Guyatt
01753 604388

Notes

- a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.
- b) Write your answers in capital letters using black ink or you may type them.
- c) If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.
- d) When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.
- e) Once you have filled in the form you must remember to sign and date it.

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Guy Storer
12 Tamar Close
Great Ashby
Stevenage
Hertfordshire
SG1 6AS

8510349001

Patents ADP number (if you know it):

Peter John Kick
10 Bulrush Close
Scarning
Dereham
Norfolk
NR19 2UE

8510356001

Patents ADP number (if you know it):

Reminder

Have you signed the form?

Patents ADP number (if you know it):

MULTIPLE NETWORK ACCESS

Background to the invention

This invention relates to techniques for access to multiple computer networks through multiple firewalls.

The invention is particularly although not exclusively concerned with enabling support staff to access multiple networks, to enable them to diagnose and fix problems.

The purpose of a firewall is to protect a computer system or network from external attacks. A firewall allows objects inside the firewall to access objects outside, but prevents objects outside the firewall from accessing objects inside it, unless they have been specifically granted access. Usually, access is granted only to a specified set of IP (Internet Protocol) addresses recognised by the firewall as having access permission.

One known method of enabling support staff to access a customer's network inside a firewall is to grant access through the firewall to one or more specified workstations. However, this has the disadvantage that only the specified workstations may be used, which causes problems if support staff are mobile and wish to use other workstations. Also, there are problems with this method if the customer's network uses NAT (Network Address Translation), preventing name to IP address resolution by traditional methods.

Another known method is to connect the support workstations directly to the customer's network, so that the workstations are inside the firewall. However, this means that only these

THIS PAGE BLANK (USPTO)

particular workstations may be used, and each workstation is limited to use with the particular customer.

The object of the present invention is to overcome these problems.

Summary of the invention

According to the invention, a computer system comprises first and second networks, the second network being protected by a firewall; wherein:

- a) the first network includes a first terminal server, which is granted permission to access the second network through the firewall;
- b) the second network includes a second terminal server, including a number of application programs that can be run remotely; and
- c) a user on the first network who has successfully logged on to the first terminal server is then enabled to log on to the second terminal server through the first terminal server, and may then remotely run application programs in the second server.

It can be seen that the invention enables an authorised user to access the second network from any workstation on the first network. However, firewall access needs to be granted only to the first server.

In the case of a support system, the first network may belong to the IT support service provider, and the second network may be a customer's network. The application programs on the second server may comprise tools for diagnosing and repairing faults on the customer's network.

THIS PAGE BLANK (USPTO)

Brief description of the drawings

Figure 1 shows a computer system, comprising an IT support service provider's network connected to a number of customers' networks.

Figure 2 is a flowchart showing the operation of the system.

Description of an embodiment of the invention

One embodiment of the invention will now be described by way of example with reference to the accompanying drawings.

Figure 1 shows a computer system, comprising a IT support service provider's network 10 connected to a number of customers' networks 11, by way of a direct network connection or an external network 12 such as the Internet. The IT support service provider's network 10 includes a number of support workstations 13, and a terminal server cluster 14. Each of the customers' networks 11 includes a firewall 15, to protect it from external attacks, and a terminal server cluster 16, located on the inside of the firewall.

In the present embodiment, the terminal servers 14 and 16 run Microsoft Windows 2000 Server or Advanced Server, with Microsoft Terminal Services enabled in application mode. With Terminal Services, terminal emulation software running on a client system provides remote access to a server-based Windows 2000 desktop. The terminal emulation software sends keystrokes and mouse movements to the server and sounds from the server to the workstation. The server does all application execution, data processing and data storage

THIS PAGE BLANK (USPTO)

locally and passes back only the display updates to the client. This reduces the network bandwidth requirements between the server and client. In addition, display information is cached at the client side to improve efficiency. Users can gain access to Terminal Services via TCP/IP, through almost any network connection medium. The end user experience is almost identical to logging on to the server directly.

As shown, in this embodiment there are two terminal servers 14 on the service provider's network. The multiple terminal servers share the system load utilising "Network Load Balancing", and provide resilience in the event of a server failure. Similarly, more than one terminal server 16 may be provided on each of the customers' networks.

The terminal servers 14 on the service provider's network are given firewall permissions on each of the firewalls 15, enabling a connection to be made, utilising TCP port 3389 (Remote Desktop Protocol), to the terminal servers 16 on the customers' networks. This enables a remote desktop session to be run on a server on a customer's network from any of the workstations 13 on the service provider's network, via the terminal server 14 on the service provider's network.

The operation of the system will now be described with reference to the flow chart in figure 2.

(Step 21) To use the system, a user (e.g. a helpdesk agent) connects to a predetermined web page, by way of a conventional web browser, and then clicks on a link in that page to initiate the connection. The web page may be hosted on the terminal servers 14, or on some other web server. This causes

THIS PAGE BLANK (USPTO)

a log-on request to be sent to one of the terminal servers 14. Connections are balanced between the two servers 14 according to load.

(Step 22) The terminal server 14 presents the user with a conventional log-on window, allowing the user to enter his or her user name and password. The terminal server 14 checks that the user is authorised, and that the password is valid. If so, the user is logged on to the server.

(Step 23) Once logged on to the terminal server 14, a terminal server session is opened within the user's web browser, and presents a web page offering connections to those customers for which this particular user has access permission. The permitted connections are conveniently presented as a drop-down list or combo box from which the user can select.

(Step 24) When the user selects a customer, a connection is made to the terminal server 16 in the selected customer's network. The terminal server 16 presents the user with a conventional log-on window, allowing the user to enter his or her user name and password. The terminal server 16 checks that the user is authorised, and that the password is valid. If so, the user is logged on to this server.

(Step 25) Once logged on to the terminal server 16, the user can perform the same operations from within the terminal server session as they would from a workstation connected directly to the customer's network 11. In particular, the user can run support applications for diagnosing and repairing faults on the customer's network. These include GUI versions of a number of command line utilities such as Ping, enabling these to be run without a command prompt.

THIS PAGE BLANK (USPTO)

The terminal server 16 may provide a custom interface for each user, allowing each user access to only a predetermined set of applications that they have been given permission to use. The custom interface provides complete access control of all applications without the need for Group Policies to lock down the user desktop, ensuring that the system can be implemented without modification of the existing configuration.

Applications are made available by placing shortcuts in a dedicated folder and setting relevant NTFS permissions (group or individual) on the shortcut. The custom interface reads the contents of the folder and, if the user has rights to an application, displays an icon for that application in a panel on the custom interface window. The user can then launch an application by clicking on its icon. A log file is maintained with a record of all applications launched, including the time and user name.

The user can switch between multiple terminal server sessions and local desktop as required. Remote control of a session is also possible to enable training or additional help if required.

The advantages of the system described above can be summarised as follows.

- The user is not restricted to a particular workstation, but may be at any workstation 13 on the service provider's network 10.
- The system is secure, in that Terminal Services Remote Desktop Protocol uses RSA Security's RC4 cipher, a stream cipher designed to efficiently encrypt small amounts of

THIS PAGE BLANK (USPTO)

varying size data. Access is restricted to authorised users only, and those users can only run permitted applications within the customer's network.

- The workstations 13 require no special configuration.
- No special software is required at the workstations 13; access is through a conventional web browser, such as Microsoft Internet Explorer version 4 or above.
- Support applications need to be installed only on the terminal servers 16, and not on the workstations 13.
- It removes problems associated with NAT (Network Address Translation).
- It reduces firewall problems caused by variations in TCP and UDP ports used by different applications. In the system described above, the terminal servers use only TCP port 3389 to communicate between the client session and the server, regardless of the application being run.
- It helps to reduce network traffic, since the only network traffic being passed over the link will be screen updates and keyboard/mouse information as opposed to application data.

Possible modifications

It will be appreciated that many modifications may be made to the system described above without departing from the principle of the present invention.

For example, different server software and different network configurations may be used.

THIS PAGE BLANK (USPTO)

CLAIMS

1. A computer system comprising first and second networks, the second network being protected by a firewall, wherein:
 - a) the first network includes a first terminal server, which is granted permission to access the second network through the firewall;
 - b) the second network includes a second terminal server, including a number of application programs that can be run remotely; and
 - c) a user on the first network who has successfully logged on to the first terminal server is then enabled to log on to the second terminal server through the first terminal server, and may then remotely run application programs in the second server.
2. A system according to claim 1 wherein, after the user has logged on to the first terminal server, the first terminal server presents the user with a list of second networks that the user is permitted to access, allowing the user to select only from that list.
3. A system according to claim 1 or 2 wherein, after the user has logged on to the second terminal server, the second terminal server presents the user with a list of application programs that the user is permitted to launch, allowing the user to select only from that list.
4. A computer system substantially as hereinbefore described with reference to the accompanying drawings.
5. A method of providing remote access to a computer network through a firewall, substantially as hereinbefore described with reference to the accompanying drawings.

THIS PAGE BLANK (USPTO)

ABSTRACT

A computer system comprises first and second networks, the second network being protected by a firewall. The first network includes a first terminal server, which is granted permission to access the second network through the firewall. The second network includes a second terminal server, including a number of application programs that can be run remotely. A user on the first network who has successfully logged on to the first terminal server is then enabled to log on to the second terminal server through the first terminal server, and may then remotely run application programs in the second server. The invention finds particularly application in enabling support staff to access multiple networks, to enable them to diagnose and fix problems.

THIS PAGE BLANK (USPTO)

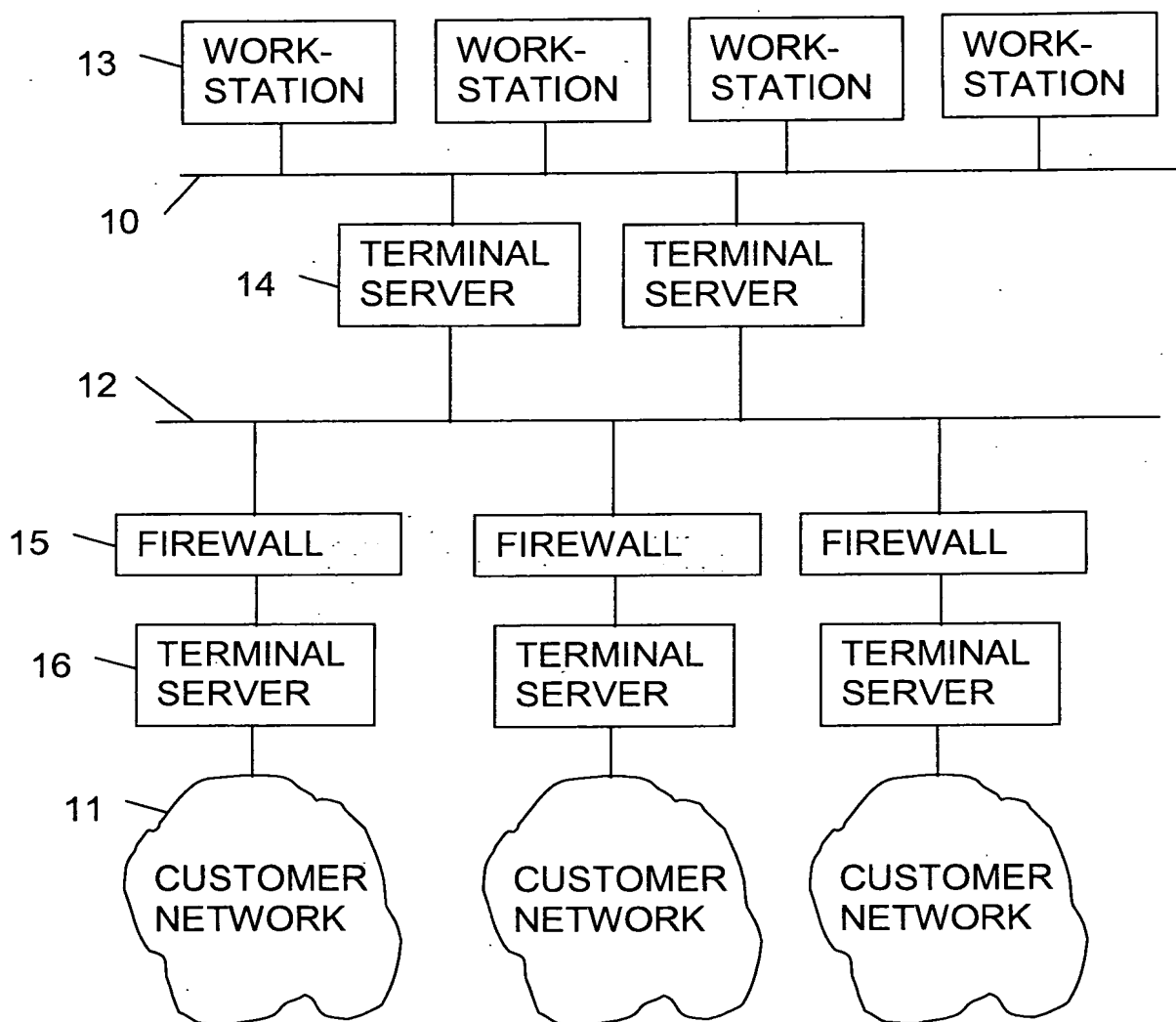


FIG. 1

THIS PAGE BLANK (USPTO)

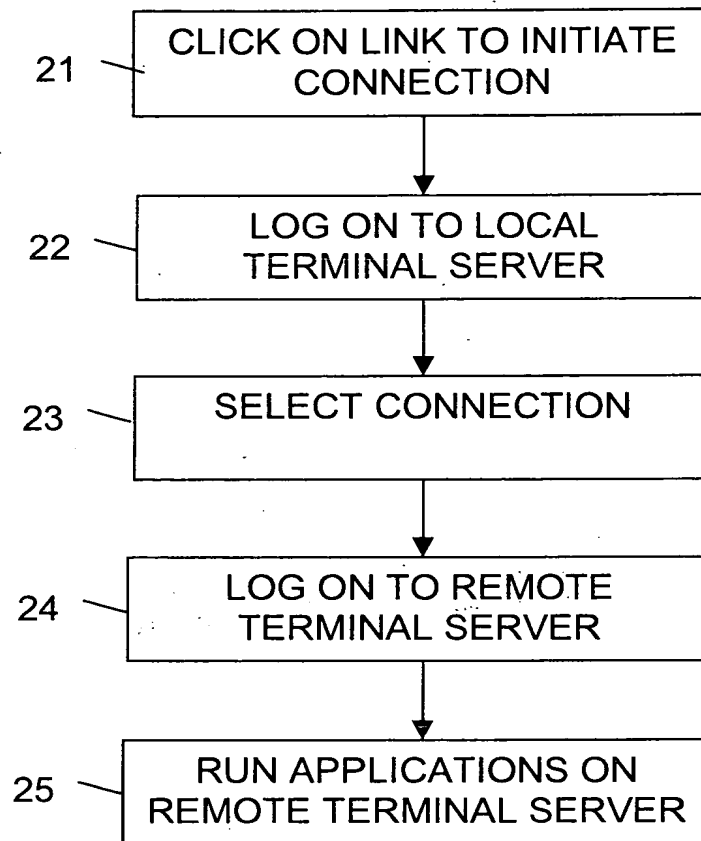


FIG. 2

THIS PAGE BLANK (USPTO)